

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P36197-P0	FOR FURTHER ACTION See Form PCT/IPEA/416	
International application No. PCT/JP2004/016643	International filing date (day/month/year) 10 November 2004	Priority date (day/month/year) 14 November 2003
International Patent Classification (IPC) or national classification and IPC Int. Cl. H04L9/16(2006.01), G11B20/10(2006.01)		
Applicant Matsushita Electric Industrial Co., Ltd.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 3 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
 - a ☒ (sent to the applicant and to the International Bureau) a total of 12 sheets, as follows:
 - ☒ sheets of the description, claims and /or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

OMISSION

4. This report contains indications relating to the following items:

- ☒ I Basis of the report
- ☐ II Priority
- ☐ III Non-establishment of opinion with regard to novelty, inventive step or industrial applicability
- ☐ IV Lack of unity of invention
- ☒ V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ VI Certain documents cited
- ☐ VII Certain defects in the international application
- ☐ VIII Certain observations on the international application

Date of submission of the demand 05 September 2005	Date of completion of this report 08 February 2006
Name and mailing address of the IPEA/JP Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

I. Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

OMISSION

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

☒ the description:
pages 1-5, 13-20, as originally filed/furnished
pages 6-12, received by this Authority on 05 September 2005

☒ the claims:
Nos. 1-6, received by this Authority on 05 September 2005

☒ the drawings:
pages 1-4, as originally filed/furnished

3. ☒ The amendments have resulted in the cancellation of:

☒ the claims, Nos. 7, 8

OMISSION

V. Reasoned statement under Rule 12 (PCT Article 35(2)) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims 1-6	YES
	Claims NONE	NO
Inventive Step(IS)	Claims 3-6	YES
	Claims 1, 2	NO
Industrial Applicability (IA)	Claims 1-6	YES
	Claims NONE	NO

2. CITATIONS AND EXPLANATIONS (Rule70.7)

Reference 1: JP 2003-115830 A (Victor Company of Japan, Ltd.), 18 April, 2003, Par. Nos. [0039], [0045]-[0047], [0055], [0060]-[0061] & US 2003/065925 A1 & EP 1300843 A2

Reference 2: JP 2002-150698 A (Pioneer Electronic Corp.), 24 May, 2002, Par. Nos. [0001], [0003], [0004], [0042] & US 2002/054681 A1

Reference 3: JP 2002-170336 A (Hitachi, Ltd.), 14 June, 2002, Par. Nos. [0025]-[0027] (Family: none)

The inventions according to Claims 1 and 2 have no inventive step in view of References 1 and 2. Reference 1 describes that a key is calculated on the basis of SEED that is written by a CPU and a media access unit number as a consecutive number that is assigned to each media access unit, and encryption and decryption is performed using the key. Reference 2 describes that an apparatus that performs scrambling, using random data that are generated as parallel data, for example by a 14-bit shift register, from an initial value which is selected from previously-prepared initial values on the basis of recording position information with respect to a disc, in which apparatus the initial value is set in the shift register, and the value set in the shift register is bit-shifted each time the random data are generated.

It is easy for a person skilled in the art to apply the invention as described in Reference 2 to the encryption and decryption in the invention as described in Reference 1. As it is a well-known matter that, in an encrypting device using a shift register, the initial value that is set in the shift register is used as a key, it is apparent to a person skilled in the art that, in an apparatus in which the invention as described in Reference 2 is applied to Reference 1, when the top of a media access unit is to be encrypted or decrypted, a key that is calculated based on the SEED and the media access unit number is set in the shift register as an initial value, and when other data are to be encrypted or decrypted, the value that is set in the shift register is bit-shifted and will be set in the shift register like the initial value.

Further, in the invention as described in Reference 2, the bit length of the parallel data is mere matter of design variation. The applicant says in the written reply that one byte of data are output in one cycle, but Reference 2 does not include such descriptions.

The inventions according to Claims 3 to 6 have novelty and inventive step. Constructions like the inventions as defined in these claims are not described in any of References 1 to 3, nor obvious to a person skilled in the art.

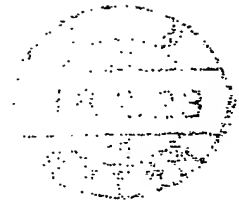
特許協力条約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第12条、法施行規則第56条）

〔PCT36条及びPCT規則70〕



出願人又は代理人 の書類記号 P36197-P0	今後の手続きについては、様式PCT/IPEA/416を参照すること。	
国際出願番号 PCT/J P 2004/016643	国際出願日 (日.月.年) 10.11.2004	優先日 (日.月.年) 14.11.2003
国際特許分類 (IPC) Int.Cl. H04L9/16(2006.01), G11B20/10(2006.01)		
出願人 (氏名又は名称) 松下電器産業株式会社		

<p>1. この報告書は、PCT35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。 法施行規則第57条（PCT36条）の規定に従い送付する。</p> <p>2. この国際予備審査報告は、この表紙を含めて全部で <u>3</u> ページからなる。</p> <p>3. この報告には次の附属物件も添付されている。</p> <p>a. <input checked="" type="checkbox"/> 附属書類は全部で <u>12</u> ページである。</p> <p><input checked="" type="checkbox"/> 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（PCT規則70.16及び実施細則第607号参照）</p> <p><input type="checkbox"/> 第I欄4.及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙</p> <p>b. <input type="checkbox"/> 電子媒体は全部で _____（電子媒体の種類、数を示す）。 配列表に関する補充欄に示すように、電子形式による配列表又は配列表に関連するテーブルを含む。 （実施細則第802号参照）</p> <p>4. この国際予備審査報告は、次の内容を含む。</p> <p><input checked="" type="checkbox"/> 第I欄 国際予備審査報告の基礎</p> <p><input type="checkbox"/> 第II欄 優先権</p> <p><input type="checkbox"/> 第III欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成</p> <p><input type="checkbox"/> 第IV欄 発明の単一性の欠如</p> <p><input checked="" type="checkbox"/> 第V欄 PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明</p> <p><input type="checkbox"/> 第VI欄 ある種の引用文献</p> <p><input type="checkbox"/> 第VII欄 国際出願の不備</p> <p><input type="checkbox"/> 第VIII欄 国際出願に対する意見</p>	
---	--

国際予備審査の請求書を受理した日 05.09.2005	国際予備審査報告を作成した日 08.02.2006	
名称及びあて先 日本国特許庁 (IPEA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 中里 裕正	5 S 9 3 6 4
電話番号 03-3581-1101 内線 3546		

様式PCT/IPEA/409 (表紙) (2005年4月)

第I欄 報告の基礎

1. 言語に関し、この予備審査報告は以下のものを基礎とした。

- ☒ 出願時の言語による国際出願
☐ 出願時の言語から次の目的のための言語である _____ 語に翻訳された、この国際出願の翻訳文
☐ 国際調査 (PCT規則12.3(a)及び23.1(b))
☐ 国際公開 (PCT規則12.4(a))
☐ 国際予備審査 (PCT規則55.2(a)又は55.3(a))

2. この報告は下記の出願書類を基礎とした。(法第6条(PCT14条)の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。)

☐ 出願時の国際出願書類

☒ 明細書

第 1-5, 13-20 _____ ページ、出願時に提出されたもの

第 6-12 _____ ページ*, 2005.09.05

第 _____ ページ*, _____ 付けで国際予備審査機関が受理したもの

☒ 請求の範囲

第 _____ 項、出願時に提出されたもの

第 _____ 項*, PCT19条の規定に基づき補正されたもの

第 1-6 _____ 項*, 2005.09.05

第 _____ 項*, _____ 付けで国際予備審査機関が受理したもの

☒ 図面

第 1-4 _____ ページ/図、出願時に提出されたもの

第 _____ ページ/図*, _____

第 _____ ページ/図*, _____ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル

配列表に関する補充欄を参照すること。

3. ☒ 補正により、下記の書類が削除された。

☐ 明細書 第 _____ ページ

☒ 請求の範囲 第 7,8 _____ 項

☐ 図面 第 _____ ページ/図

☐ 配列表 (具体的に記載すること)

☐ 配列表に関連するテーブル (具体的に記載すること)

4. ☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c))

☐ 明細書 第 _____ ページ

☐ 請求の範囲 第 _____ 項

☐ 図面 第 _____ ページ/図

☐ 配列表 (具体的に記載すること)

☐ 配列表に関連するテーブル (具体的に記載すること)

* 4. に該当する場合、その用紙に "superseded" と記入されることがある。

第V欄 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、
それを裏付ける文献及び説明

1. 見解

新規性 (N)	請求の範囲 1-6	有
	請求の範囲	無
進歩性 (IS)	請求の範囲 3-6	有
	請求の範囲 1, 2	無
産業上の利用可能性 (IA)	請求の範囲 1-6	有
	請求の範囲	無

2. 文献及び説明 (PCT規則70.7)

文献1: JP 2003-115830 A (日本ビクター株式会社) 2003.04.18
第39, 45-47, 55, 60-61段落 & US 2003/065925 A1 & EP 1300843 A2

文献2: JP 2002-150698 A (パイオニア株式会社) 2002.05.24
第1, 3, 4, 42段落 & US 2002/054681 A1

文献3: JP 2002-170336 A (株式会社日立製作所) 2002.06.14
第25-27段落 (ファミリーなし)

請求の範囲1, 2に係る発明は、文献1, 2により進歩性を有しない。文献1には、中央処理装置が書き込むSEEDと、メディアアクセスユニット毎に付与される連続的な番号であるメディアアクセスユニットナンバーとに基づいて鍵を算出し、当該鍵を用いて暗号化及び復号を行うことが記載されている。文献2には、予め用意した初期値からディスクに対する記録位置情報に基づいて選択した初期値から例えば14ビットのシフトレジスタを用いてパラレルデータとして発生したランダムデータを用いてスクランブルをするものにおいて、初期値をシフトレジスタに設定すると共にランダムデータを発生する毎にシフトレジスタに設定された値をビットシフトすることが記載されている。

文献2に記載された発明を文献1に記載された発明における暗号化及び復号に用いることは当業者にとって容易である。なおシフトレジスタを用いた暗号装置において、シフトレジスタに設定される初期値が鍵となることは周知の事項であるから、文献2に記載された発明を文献1に適用したものは、メディアアクセスユニットの先頭を暗号化あるいは復号するときにはSEED及びメディアアクセスユニットナンバーから算出した鍵を初期値としてシフトレジスタに設定し、それ以外のデータを暗号化あるいは復号するときにはシフトレジスタに設定された値がビットシフトにより初期値と同様にシフトレジスタに設定されるものとなることは当業者に明らかである。

また文献2に記載された発明においてパラレルデータのビット長をどのようなものとするかは設計的事項にすぎない。出願人は答弁書にて1サイクルで1byteのデータが出力されるものである旨を述べているが、文献2にそのような記載はない。

請求の範囲3-6に係る発明は、新規性・進歩性を有する。これらの請求項に係る発明のように構成することは文献1-3のいずれにも記載されておらず、当業者にとって自明なものでもない。